LA SEGURIDAD EN LAS REDES DE COMUNICACIONES

Seguridad de la información en la Red

Se puede entender la seguridad como la necesidad de proteger. En una red se deben proteger todos los equipos que posibilitan el proceso de la comunicación, las personas que producen, acceden y distribuyen los datos y finalmente la información que es considerada como uno de los activos más importantes de las organizaciones. Para mantener segura la información que viaja a través de la red esta debe cumplir con tres requisitos:

Imagen 1.

Imagen 2.

1. **Integridad**: Requiere que los recursos sean modificados por quienes están autorizados y que los métodos y los procesamientos de la información sean salvaguardados en su totalidad y con exactitud.
2. **Confidencialidad**: Se debe garantizar que la información sea accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación.
3. **Disponibilidad**: Se requiere que la información esté disponible en el momento exacto para quienes están autorizados a acceder a ella.

Ataques a la seguridad de la red

Dentro del proceso de comunicación existen dos tipos de ataques a la red de transmisión de datos a saber:

- **Ataques pasivos**: Son oidores o monitoreos de las transmisiones. El objetivo de quienes realizan ese tipo de ataque es obtener la información que se está transmitiendo. En este tipo de ataque se pueden encontrar:

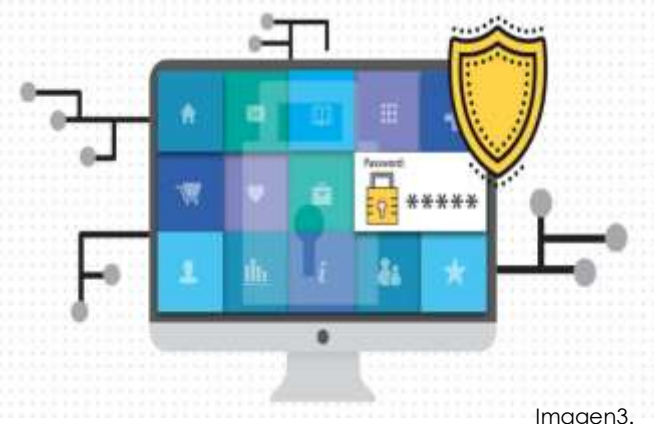
- ✓ **Divulgación del contenido de un mensaje**: es un tipo de ataque pasivo por medio del cual el atacante se entera de la información transmitida; como por ejemplo escuchar una llamada telefónica, leer un correo electrónico abierto.
- ✓ **Análisis de Tráfico**: Este tipo de ataque pasivo se realiza cuando el atacante puede determinar la localización e identidad de quienes se están comunicando y determinar el mensaje que está siendo transmitido aun cuando esté protegido por medio de cifrado.

- **Ataques activos**: Suponen modificación de los datos o creación de flujos de datos falsos.

  Dentro de este tipo de ataques se pueden encontrar:

- ✓ **Enmascaramiento**: Es un tipo de ataque activo que tiene lugar cuando una entidad pretende suplantar a otra para obtener información confidencial.
- ✓ **Repetición**: Se realiza con la captura de unidades de datos que se vuelven a retransmitir para producir efectos no autorizados.
- ✓ **Modificación de Mensajes**: Se modifican los mensajes para producir efectos no autorizados.
- ✓ **Denegación de Servicios**: Previene o inhabilita el uso normal de las facilidades de comunicación, usualmente se hace para obtener un fin específico o para obtener perturbaciones sobre la red desmejorando su rendimiento o incluso inhabilitando la misma.

Herramientas de seguridad



Imaaen3.

Existen métodos o herramientas tecnológicas que ayudan a las organizaciones a mantener segura la red. Estos métodos, su utilización, configuración y manejo dependen de los requerimientos que tenga la organización para mantener la red en un funcionamiento óptimo y protegido contra los diferentes riesgos. Los más utilizados son:

Autenticación: Identifica quien solicita los servicios en una red. Esta no hace referencia solo a los usuarios sino también a la verificación de un proceso de software.

Autorización: Indica que es lo que un usuario puede hacer o no cuando ingresa a los servicios o recursos de la red. La autorización otorga o restringe privilegios a los procesos y a los usuarios.

Auditoria: Para analizar la seguridad de una red y responder a los incidentes de seguridad, es necesario hacer una recopilación de datos de las diferentes actividades que se realizan en la red, a esto se le llama contabilidad o auditoria. Con normas de seguridad estrictas la auditoria debe incluir una bitácora de todos los intentos que realiza un usuario para lograr conseguir la autenticación y autorización para ingresar a la red. También debe registrarse los accesos anónimos o invitados a los servidores públicos, así como registrar los intentos de los usuarios para cambiar sus privilegios.

Cifrado: Es un proceso que mezcla los datos para protegerlos de su lectura, por parte de otro que no sea el receptor esperado. Un dispositivo de cifrado encripta los datos colocándolos en una red. Esta herramienta constituye una opción de seguridad muy útil, ya que proporciona confidencialidad a los datos. Se recomienda el cifrado de datos en organizaciones cuyas redes se conectan a sitios privados a través de Internet mediante redes privadas virtuales.

Filtros de paquete: Se pueden configurar en routers2 o servidores para rechazar paquetes de direcciones o servicios concretos. Los filtros de paquete ayudan a proteger recursos de la red del uso no autorizado, destrucción, sustracción y de ataques de denegación del servicio. Las normas de seguridad deben declarar si los filtros implementan una de las siguientes normas:

· Denegar tipos específicos de paquetes y aceptar todo lo demás
· Aceptar tipos específicos de paquetes y denegar todo lo demás.

Firewalls3: Es un sistema o combinación de sistemas, que exige normas de seguridad en la frontera entre dos o más redes.

Vlan: En una red LAN se utilizan los switches4 para agrupar estaciones de trabajo y servidores en agrupaciones lógicas. En las redes, las VLAN se usan para que un conjunto de usuarios en particular se encuentre agrupado lógicamente. Las VLAN permiten proteger a la red de potenciales problemas conservando todos los beneficios de rendimiento.

Detección de Intrusos: Una intrusión es cualquier conjunto de acciones que puede comprometer la integridad, confidencialidad o disponibilidad de una información o un recurso informático. Los intrusos pueden utilizar

debilidades en la arquitectura de los sistemas y el conocimiento interno del sistema operativo para superar el proceso normal de autenticación. . Una intrusión significa:

· Acceder a una determinada información.
· Manipular cierta información.
· Hacer que el sistema no funcione de forma segura o inutilizarlo.

Activos

Un activo es todo aquel elemento que se encuentra inmerso en el proceso de la comunicación. Desde la misma información, el emisor, el medio y el receptor, como en la economía, también en la seguridad de una red. Estos activos poseen un valor para la organización, en mayor o menor medida, más o menos relevantes en el proceso. Son tres los elementos denominados como activos en el proceso de la comunicación:

- **La información**: todos los datos que se encuentren en cualquiera de las presentaciones.
- **Los equipos**: el hardware, el software, e infraestructura organizacional que permite el trasporte de los datos
- **Las personas**: producen, distribuyen y acceden a la información.

Imagen4.

Vulnerabilidades y Amenazas

Imagen5.

Los activos en una red a menudo contienen fallas o huecos en la seguridad. Estos huecos o vulnerabilidades desembocan en un problema de seguridad y representan un riesgo para los activos.

Una amenaza es cualquier evento de seguridad capaz de utilizar una vulnerabilidad para atacar o dañar un activo. Las amenazas se pueden dividir en tres grupos:

- **Naturales**: cualquier evento de seguridad producido por un fenómeno como terremoto, incendio, inundación, etc.
- **Intencionales**: eventos de seguridad causados deliberadamente sobre un activo con la firme intención de causar daños o perdida, fraudes, etc.
- **Involuntarias**: eventos de seguridad producidos accidentalmente

Riesgos y medidas de seguridad

Imagen6.

Un riesgo es la probabilidad de que ocurra un evento en contra de la seguridad de la red o uno de sus activos causando daños o pérdidas. Un análisis de riesgos permitirá a la organización especificar cuales riesgos son más probables de ocurrencias, cuáles serán más destructivos y cuáles serán los más urgentes de minimizar. Las medidas de seguridad son las acciones que toma una organización para disminuir los riesgos de seguridad.

Las medidas de seguridad se dividen en:

- **Preventivas**: son las medidas que tienden a disminuir el riesgo de que una amenaza ocurra antes de producirse.
- **Perceptivas**: estas medidas consisten en realizar acciones que revelen riesgos no detectados.
- **Correctivas**: son las medidas que se toman cuando ha ocurrido una amenaza.

Análisis de seguridad de la red

Identificar los activos de la red

Para identificar los activos de una red se deben tener en cuenta los diferentes tipos de activos que se encuentran en ella:

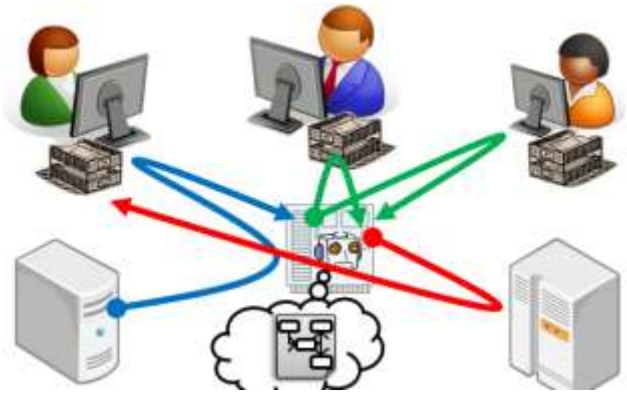


Imagen7.

- **Los equipos:** son todos aquellos elementos de hardware que hacen posible la comunicación de datos en la red y la infraestructura de la misma. Identificar estos equipos de acuerdo a sus características como equipos activos y pasivos es determinante a la hora de valorar el riesgo al que se encuentran expuestos cada uno de estos activos. Entre estos equipos se tienen terminales de usuario, switches, routers, centrales telefónicas, firewalls, etc. Cada uno de estos tiene unas características específicas y una funcionalidad en la red que determinan su importancia y el impacto que produciría un fallo en alguno de estos equipos. Por ejemplo, la mala configuración del firewall de la red permitiría el acceso a servicios no autorizados para empleados o personas externas a la red accediendo a información a la que no se encuentran autorizados, también el firewall permitiría el paso de virus o software malicioso capaz de atacar a los diferentes tipos de usuarios y su información.

- **El software**: se debe tener un control con el software debido a que en aplicaciones se pueden encontrar huecos de seguridad por donde se pueden producir ataques que se propagan al resto de la red como virus y accesos a puertas traseras o puertos abiertos que deja algún tipo de software y especial cuidado con las aplicaciones de uso abierto que en la mayoría de casos no presentan ningún control y menos un soporte adecuado. En aplicaciones de uso específico en la organización se debe tener en cuenta el tipo de información que esta suministra, procesa y distribuye y quienes tienen acceso a ella.

- **El personal**: se debe identificarse como un activo debido a que son quienes ejecutan los procesos para mantener la continuidad del negocio y son quienes tienen acceso a la red y a su información con mayor o menor restricción. Determinar qué tipos de permisos tienen cada usuario y grado de confianza que representa un empleado en la organización ayudará a que las medidas de seguridad sean más de tipo preventivo que correctivo. Un empleado de un departamento de ventas que tiene permiso para acceder a la nómina y cambiar los datos de salario representaría una amenaza de seguridad o un mensajero que tiene acceso a la información específica de un nuevo producto podría entregar esa información a la competencia generando así una fuga y una falla de seguridad.

- **La información**: debe clasificarse de acuerdo al nivel de importancia que representa en la continuidad del negocio. Los niveles de clasificación de la información determinarán el grado de protección al que esta debe estar sometida y quien o quienes pueden tener acceso a ella. No tendría efectividad proteger a los diferentes activos de la red si la información que por ella viaja está expuesta a cualquiera que quisiera acceder a ella.

Análisis de riesgos

Existen diferentes métodos de análisis de riesgos de seguridad. Métodos cuantitativos y métodos cualitativos. El uso de uno u otro depende de la organización y la efectividad que cada uno de estos representa.

En un enfoque cuantitativo se calculan las perdidas en valor monetario que generaría la ocurrencia de un evento de seguridad, es decir, una amenaza. En esta metodología se toman los valores de los activos como punto de partida, los costos que generaría una falla de estos activos para solucionar un problema y las pérdidas que representan para la organización. Un activo puede contener varios riesgos implícitos, cada uno con unas consecuencias, medidas de pérdidas y costos totalmente diferentes. En este orden, para cada riesgo en el que se encuentre un activo es necesario calcular los distintos costos que se generan por la acción de un evento de seguridad, lo que en una organización donde la cantidad de activos es considerablemente alta, este enfoque resultaría más dispendioso y menos factible de realizar, puesto que, la cantidad de recursos humanos y de tiempo en el que la totalidad de cálculos se pueden realizar es cada vez mayor, y con el paso del tiempo un activo puede ir perdiendo su valor lo que significaría que al final de todos los cálculos estos ya no serían de utilidad o estarían erróneos para un instante determinado. En una evaluación de riesgos cualitativa, no se asignan los

valores monetarios a los activos y tampoco se relacionan sus costos en cuanto a la ocurrencia de un evento de seguridad.
En este enfoque, mediante un estudio cuidadoso, se priorizan los activos asignándoles un valor relativo de acuerdo a la función que cumplan dentro de la red de la organización. En este método se hace necesario que los clientes internos de la organización participen en forma directa en el proceso. Para tal fin, por medio de encuestas que permitan determinar el valor relativo de los activos se hace más sencilla una aceptación de la importancia de cada activo para la organización y los riesgos a los que se encuentra expuesto.

La finalidad especifica del análisis de riesgos, en cualquiera de los enfoques, cuantitativo, cualitativo o híbrido, es dar prioridad a los riesgos que mayor impacto causarían en la organización para así determinar cuáles controles son más importantes implementar.

Matriz de control

Una matriz de control es un sistema que nos permite priorizar riesgos. Los campos que se deben considerar para generar la matriz de control son:

- **Activo**: Corresponde al activo determinado en el estudio.
- **Amenaza**: Evento en contra de la seguridad
- **Consecuencia**: Efecto que causaría la ocurrencia de la amenaza.
- **Probabilidad de ocurrencia**: Es la probabilidad estimada de que ocurra una amenaza. El valor se encuentra entre 0 y 1.
- **Impacto**: Efecto que causa un evento de seguridad en la organización con respecto a perdidas y los traumas a los procesos. De acuerdo con la guía de Administración de Riesgos de Seguridad de Microsoft cada uno de los activos tiene un valor específico de importancia dentro de la red que permite valorar su jerarquía. Con este valor se puede determinar el impacto que causaría la ocurrencia de un evento sobre el activo. Para la matriz de control la organización podría modificar este rango, que para Microsoft se encuentra en 0 y 5, al rango entre 0 y 10, siendo 0 el valor menos importante que se puede asignar a un activo y 10 el mayor.
- **Capacidad de reacción**: es la rapidez para resolver un problema que se presenta al ocurrir un evento de seguridad de acuerdo al criterio propio, ya que depende de los recursos humanos, físicos, operativos y económicos de la organización. El rango se encuentra entre 0 y 10, siendo 0 la mínima y 10 la mayor capacidad de solucionar un problema.
- **Vulnerabilidad**: es el estado en el que se encuentra un activo con respecto a una amenaza

Estimación de la Vulnerabilidad

La matriz de control permite estimar los grados de vulnerabilidad con el fin de priorizar los riesgos que requieren de controles más rápidos y efectivos para determinar las acciones de seguridad adecuadas y .la implementación de controles a fin de brindar protección contra dichos riesgos. El proceso de estimación de la vulnerabilidad en el método utilizado se realiza con los datos de probabilidad de ocurrencia, impacto y capacidad de reacción con el fin de dar un valor cuantificable que permite a su vez dar el grado de vulnerabilidad que puede corresponder a uno de cuatro estados: Peligro, indefenso, vulnerable y preparado.

Peligro: es el estado más crítico que indica que el riesgo es inminente y sucederá, en cuyo caso la capacidad de reacción para superar el evento de seguridad es muy baja lo que causará grandes traumas y perdidas. En este estado los controles deben ser rigurosos para cambiar a otro estado menos crítico.

Indefenso: indica que al presentarse un evento de seguridad será difícil reaccionar para salvaguardarlo debido a que la inexistencia de controles y políticas sobre estos riesgos dificultan el proceso.

Vulnerable: es un estado de mucho riesgo y cuidado que indica que la capacidad de reacción en caso de suceder un evento de seguridad es relativamente baja y deben aplicarse controles con el fin de evitar que su estado se vuelva peligro.

Preparado: es un estado que se podría llamar ideal siempre y cuando los controles y políticas de seguridad que se apliquen sean continuos y ayuden a mantener siempre controlados los riesgos.

Requisitos de la seguridad

Con la priorización de riesgos, la organización ya está en capacidad de determinar cuáles son los requisitos que necesitan para llevar a cabo un plan de contingencia a fin de minimizar los riesgos y en qué aspectos debe tener mayor énfasis. Dentro de los requisitos a tener en cuenta están:

- **Entrenamiento a los usuarios en cuanto a las normas, procedimientos y objetivos de acceso a la red**: Este entrenamiento permitirá disminuir las vulnerabilidades propias al factor humano que corresponden a un gran porcentaje dentro de los riesgos en las organizaciones.

- **Protección de los equipos de la red**: Permiten disminuir las vulnerabilidades propias del factor tecnológico.
- **Procedimientos**: permiten mantener minimizados los riesgos a los que la organización se expone con sus activos.

Teniendo en cuenta estos tres factores, se debe determinar el plan de seguridad y las políticas respectivas, que permitan disminuir las vulnerabilidades y fortalecer los estados ideales de los riesgos a los que se encuentran expuestos los activos de la red.

Controles

Plan de seguridad

Imagen8.

Un plan de seguridad debe contemplar diferentes aspectos acerca de cómo se mantendrá la seguridad en la red. Este plan debe contener:

- **Tiempo, Gente y Recursos**: Un plan de seguridad debe ejecutarse de forma permanente. No existe un tiempo limitado o específico para ejecutar una asignación de esta política, puesto que el mejoramiento en la prestación de los servicios y minimización de las amenazas a la seguridad debe realizarse de forma continua. Se contemplan en este plan los servicios que presta o deberá prestar la red teniendo en cuenta que estos pueden cambiar, aumentar o en caso dado disminuir por la entrada de nuevos servicios, lo que implica que las políticas de seguridad que se desprendan de este plan puedan cambiar a medida que los servicios cambien. La puesta en marcha de este plan de seguridad dependerá de la apropiación que hagan de este todos los involucrados en su desarrollo, uso y beneficiarios del mismo.

- **Topología de la red y servicios**: Un plan de seguridad debe contener de manera detallada la topología de la red, explicación de los servicios que la red presta tanto a usuarios internos como externos, detalles de dependencias y tecnologías de comunicación.

- **Especificación de Funciones**: Las funciones de los usuarios deben estar bien especificadas con el fin de dar responsabilidad a cada uno en los procesos que le son pertinentes en cuanto a la seguridad

de la red. Estas funciones deben desprenderse de las políticas generadas a partir de este plan y deben contemplar procesos de actuación concreta de cada uno de actores.

Se deben especificar: recursos y procesos asignados a cada usuario, definición de niveles de autorización o permisos, responsabilidades específicas y tipos de usuarios.

Políticas de seguridad.

Las políticas de seguridad son los lineamientos y formas de comunicación con los usuarios, que establecen un canal de actuación en relación a los recursos y servicios de la red. Esto no significa que las políticas sean una descripción técnica de mecanismos y tecnologías de seguridad específicas y tampoco términos legales que impliquen sanciones. Las políticas son una descripción de lo que se desea proteger y la razón por la cual debe hacerse. Estos lineamientos deben abordar aspectos como la evaluación de los riesgos, protección perimétrica, control de acceso, y normas de uso de Internet y correo electrónico, protección contra virus y copias de seguridad entre otros.

Imagen9.

No todas las organizaciones desean llevar a cabo una certificación en procesos de seguridad de la información, pero si todas, desean protegerse y proteger sus activos. La norma ISO 17799 contempla varios parámetros en los cuales se especifican de manera general un punto de partida para lograr el objetivo.

Basados en la norma se producen las políticas de seguridad para la organización, cuyo fin es generar la base de normas mínimas para el correcto desempeño en la prestación de servicios a los involucrados en el uso de la red con un mínimo de seguridad que otorgue a los usuarios la confidencialidad, integridad y disponibilidad de información que ellos necesitan. La apropiación de estas políticas debe ser hecha por parte de todos los usuarios que acceden a servicios en la red de la organización, pues de su universalización depende la disminución de riesgos y vulnerabilidades a los que la red se encuentra expuesta. Se contemplan en estas políticas los aspectos básicos de seguridad en cuanto a

comunicaciones se refiere, cuyo objetivo principal es garantizar el funcionamiento correcto y seguro de las instalaciones de la red:

- Procedimientos y responsabilidades.
- Planificación de la capacidad y aprobación de nuevos accesos o servicios en la red.
- Protección contra software malicioso.
- Mantenimiento de la información y servicios.
- Administración de red.
- Medios de almacenamiento.
- Intercambio de información.
- Control de accesos.

El seguimiento de las políticas y la consecución del plan de seguridad es responsabilidad no solo de los administradores de red, sino de todo aquel que tenga acceso a los servicios de red en mayor o menor medidas sin importar tipo de usuario, servicio o tiempo de uso del mismo.

Revisiones y actualizaciones de las políticas de seguridad

El plan de seguridad y las políticas generadas a través del mismo deben mantenerse acordes a los cambios de personal, tecnológicos y de procedimientos propios de la red con el fin de minimizar los riesgos que se pudieran generar debido a estos cambios. Por esta razón la gestión de seguridad debe mantenerse al tanto de cualquier evento ocurrido sobre la infraestructura de red que ocasione un cambio significativo. La gestión de seguridad no es solo deber de los administradores de la red o de los coordinadores. Desde el nivel más alto de administración de la organización hasta los usuarios menos concurrentes en los servicios de red se deben apropiar de este plan y políticas con el fin de generar nuevas revisiones, pautas de cambio y actualizaciones.

Imagen10.

REFERENCIAS

Ing. Jaime Alirio González, Msc, Carlos Alberto Vanegas, "La seguridad en las redes de comunicaciones", recuperado de: http://comunidad.udistrital.edu.co/revistavinculos/files/2012/12/LA-SEGURIDAD-EN-LAS-REDES-DE-COMUNICACIONES-ED5.pdf

Imágenes:

Imagen 1, recuperada de: http://blog.capacityacademy.com/2014/03/13/que-es-la-seguridad-de-la-informacion/

Imagen 2, recuperada de: https://infosegur.wordpress.com/tag/integridad/

Imagen 3, recuperada de: http://www.blog.andaluciaesdigital.es/seguridad-informatica-para-pymes/

Imagen 4, recuperada de: http://www.infodf.org.mx/index.php

Imagen 5, recuperada de: http://www.pqs.pe/tecnologia/seguridad-informatica-empresas-vulnerabilidades-sistemas

Imagen 6, recuperada de: http://seguridadinformaticaci.blogspot.com.co/

Imagen 7, recuperada de: https://docentegabrielacruz.wordpress.com/aplicacion-de-la-seguridad-informatica/unidad-1-aplica-estandares-de-proteccion-de-la-informacion/r-a-1-1-determina-riesgos-de-seguridad-informatica-con-base-en-las-caracteristicas-del-equipo-y-las-necesidades-del-usuario/

Imagen 8, recuperada de: http://www.coordinacionempresarial.com/errores-frecuentes-en-la-elaboracion-de-planes-de-seguridad-y-salud/

Imagen 9, recuperada de: http://segur-inf.blogspot.com.co/

Imagen 10, recuperada de:: http://rahabogados.com.mx/revisiones-electronicas-2017/